MINISTÉRIO DA DEFESA

MD31-P-03

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PARA O SISTEMA MILITAR DE COMANDO E CONTROLE

2023

MINISTÉRIO DA DEFESA
ESTADO-MAIOR CONJUNTO DAS FORÇAS ARMADAS

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PARA O SISTEMA MILITAR DE COMANDO E CONTROLE

3ª Edição
2023

MINISTÉRIO DA DEFESA
ESTADO-MAIOR CONJUNTO DAS FORÇAS ARMADAS

PORTARIA GM-MD Nº 5.429, DE 9 DE NOVEMBRO DE 2023.

Aprova a Política de Segurança da Informação para o Sistema Militar de Comando e Controle - MD31-P-03 (3ª Edição/2023).

O MINISTRO DE ESTADO DA DEFESA, no uso da atribuição que lhe confere o art. 87, parágrafo único, inciso I, da Constituição, tendo em vista o disposto no art. 1º, incisos II e III, do anexo I, do Decreto nº 11.337, de 1º de janeiro de 2023, no art. 18 do Decreto nº 9.637, de 26 de dezembro de 2018, e de acordo com o que consta do Processo Administrativo nº 60080.000274/2023-82, resolve:

Art. 1º Esta Portaria aprova a Política de Segurança da Informação para o Sistema Militar de Comando e Controle - MD 31-P-03 (3ª edição/2023).

Parágrafo único. A Política de que trata o caput estará disponível na Assessoria de Doutrina e Legislação (ADL) do Estado-Maior Conjunto das Forças Armadas (EMCFA) e na Plataforma de Pesquisa da Legislação da Defesa - MDLegis (<https://mdlegis.defesa.gov.br/pesquisar_normas/>).

Art. 2º Fica revogada a Portaria Normativa nº 2.327/MD, de 28 de outubro de 2015, publicada no Diário Oficial da União nº 207, de 29 de outubro de 2015, seção 1, páginas 14 e 15.

Art. 3º Esta Portaria entra em vigor em 1º de dezembro de 2023.

JOSÉ MUCIO MONTEIRO FILHO

(Publicada no D.O.U – Edição 219 – Seção 1 – Página 34, de 20 de novembro de 2023)

REGISTRO DE MODIFICAÇÕES

NÚMERO DE ORDEM	ATO DE APROVAÇÃO	PÁGINAS AFETADAS	DATA	RUBRICA DO RESPONSÁVEL

SUMÁRIO

LISTA DE DISTRIBUIÇÃO

INTERNA	
ÓRGÃOS	**EXEMPLARES**
CHEFIA DE OPERAÇÕES CONJUNTAS	1
CHEFIA DE ASSUNTOS ESTRATÉGICOS	1
CHEFIA DE LOGÍSTICA E MOBILIZAÇÃO	1
CHEFIA DE EDUCAÇÃO E CULTURA	1
ASSESSORIA DE INTELIGÊNCIA DE DEFESA	1
ASSESSORIA DE DOUTRINA E LEGISLAÇÃO - **Exemplar Mestre**	1
PROTOCOLO GERAL	1
SUBTOTAL	**7**

EXTERNA	
ÓRGÃOS	**EXEMPLARES**
ESTADO-MAIOR DA ARMADA	1
ESTADO-MAIOR DO EXÉRCITO	1
ESTADO-MAIOR DA AERONÁUTICA	1
COMANDO DE OPERAÇÕES NAVAIS	1
COMANDO DE OPERAÇÕES TERRESTRES	1
COMANDO DE OPERAÇÕES AEROESPACIAIS	1
SUBTOTAL	**6**
TOTAL	**13**

CAPÍTULO I

INTRODUÇÃO

1.1 Finalidade

A Política de Segurança da Informação para o Sistema Militar de Comando e Controle (POSIN-SISMC²) tem por finalidade estabelecer objetivos e orientações gerais de Segurança da Informação (SI), de modo a garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações no âmbito do Sistema Militar de Comando e Controle (SISMC²).

1.2 Referências

Os documentos consultados para a elaboração desta Política foram:

a) Lei n° 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados (LGPD);

b) Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação (PNSI);

c) Decreto nº 10.748, de 16 de julho de 2021, que institui a Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC);

d) Decreto n° 10.222, de 05 de fevereiro de 2022, que institui a Estratégia Nacional de Segurança Cibernética (E-Ciber);

e) Portaria GM-MD nº 5.081, de 16 de outubro de 2023, que aprova a Doutrina Militar de Defesa Cibernética - MD 31-M-07 (2ª Edição/2023);

f) Portaria Normativa nº 1.691/MD, de 05 de agosto de 2015, que dispõe sobre a Doutrina para o Sistema Militar de Comando e Controle - MD31-M-03 (3ª Edição/2015).

g) Portaria Normativa nº 2.328/MD, de 28 de outubro de 2015, que dispõe sobre a Política para o Sistema Militar de Comando e Controle - MD31-P-01 (3ª Edição/2015);

h) Portaria nº 3.781/GM-MD, de 17 de novembro de 2020, que cria o Sistema Militar de Defesa Cibernética (SMDC) e dá outras providências;

i) Portaria nº 4.511/GM-MD, de 04 de novembro de 2021, que aprova o Regulamento do Conselho Diretor do Sistema Militar de Comando e Controle (CD-SISMC²);

j) Portaria SGD/MGI n° 852, de 28 de março de 2023, que dispõe sobre o Programa de Privacidade e Segurança da Informação (PPSI);

k) Instrução Normativa EMCFA-MD n° 3, de 14 de junho de 2022, Aprova as Instruções para Elaboração e Revisão de Publicações Padronizadas do Estado-Maior Conjunto das Forças Armadas - MD20-I-01 (2ª Edição/2022);

l) Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

m) Instrução Normativa GSI/PR nº 5, de 20 de agosto de 2021, que dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal;

n) Portaria GSI/PR nº 93, de 18 de outubro de 2021, que aprova o Glossário de Segurança da Informação;

o) Portaria nº 4.138/GM-MD, de 14 de agosto de 2023, que institui a Equipe de Coordenação Setorial da Defesa (ECS/Def) da Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC);

p) Norma Técnica ABNT NBR ISO/IEC 27001:2022, de 23 de novembro de 2022, Segurança da Informação, Segurança Cibernética e Proteção à Privacidade - Sistemas de Gestão da Segurança da Informação - Requisitos (3ª edição); e

q) Norma Técnica ABNT NBR ISO/IEC 27002:2022, de 05 de outubro de 2022, Segurança da Informação, Segurança Cibernética e Proteção à Privacidade - Controles de Segurança da Informação (3ª edição).

1.3 Aplicação

No âmbito do Ministério da Defesa (MD), caberá aos Comandos da Marinha, do Exército e da Aeronáutica editar, em suas respectivas áreas de atuação, atos específicos complementares para a implementação da POSIN-SISMC² de que trata esta Política.

1.4 Informação

1.4.1 As siglas, as abreviaturas e os acrônimos utilizados nesta publicação seguem o previsto no Manual de Abreviaturas, Siglas, Símbolos e Convenções Cartográficas das Forças Armadas – MD33-M-02 (4ª edição/2021).

1.4.2 No caso de siglas, abreviaturas e acrônimos não previstos no Manual MD33-M-02 (4ª edição/2021), em face da temática e da especificidade abordadas nesta publicação, esses farão parte de uma lista, em anexo.

1.4 Aprimoramento

As sugestões para aperfeiçoamento deste documento deverão ser encaminhadas ao Estado-Maior Conjunto das Forças Armadas (EMCFA), para o seguinte endereço:

MINISTÉRIO DA DEFESA
Estado-Maior Conjunto das Forças Armadas
Assessoria de Doutrina e Legislação
Esplanada dos Ministérios
Bloco Q (Edifício Defensores da Pátria) – 4º Andar
Brasília – DF
CEP – 70049–900
adl1.emcfa@defesa.gov.br

CAPÍTULO II

CONCEITOS E DEFINIÇÕES

2.1 Considerações Iniciais

Para os efeitos da POSIN-SISMC², em que pese os termos, palavras, vocábulos e expressões expostos no Glossário das FA (MD35-G-01), serão considerados, entre outros, os conceitos e definições constantes no Glossário de Segurança da Informação do GSI/PR, a fim de buscar uma melhor compreensão com o tema "Segurança da Informação". Em especial, considerou-se:

a) **atividade crítica**: atividade que deve ser executada visando garantir a consecução dos produtos e serviços fundamentais do órgão ou entidade, de tal forma que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo;

b) **ativos de informação**: meios de armazenamento, transmissão e processamento de dados e informação, equipamentos necessários a isso (computadores, equipamentos de comunicações e interconexão), os sistemas utilizados para tal, os sistemas de informação de um modo geral, bem como os locais onde se encontram esses meios e os recursos humanos que a eles têm acesso;

c) **auditoria**: processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se elas estão de acordo com as disposições planejadas e estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas e em conformidade à consecução dos objetivos;

d) **autenticidade**: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;

e) **avaliação de conformidade**: processo sistematizado, acompanhado e avaliado, de forma a propiciar adequado grau de confiança de que um produto, processo ou serviço, ou ainda um profissional, atende a requisitos pré-estabelecidos em normas e regulamentos técnicos com o menor custo para a sociedade;

f) **confidencialidade**: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados;

g) **controle de acesso**: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Via de regra, requer procedimentos de autenticação;

h) **Conselho Diretor do Sistema Militar de Comando e Controle (CD-SISMC²):** Colegiado que tem a finalidade de assessorar, em caráter permanente e deliberativo, o Chefe do Estado-Maior Conjunto das Forças Armadas, por intermédio do Chefe de Operações Conjuntas (Ch de Op Cj) nos trabalhos relativos:

1) à concepção, organização, desenvolvimento, implementação, integração, manutenção, avaliação e evolução do SISMC²;

2) ao planejamento, direção e controle das ações de governança da tecnologia da informação e das comunicações do SISMC²; e

3) à formulação da Política de Governança de Comando e Controle, em conformidade com as diretrizes governamentais;

i) **defesa cibernética**: ações realizadas no espaço cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo MD, com as finalidades de proteger os

ativos de informação de interesse da defesa nacional, obter dados para a produção de conhecimento de inteligência e buscar superioridade sobre os sistemas de informação do oponente.

j) **disponibilidade**: propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

k) **Equipe de Coordenação Setorial Defesa (ECS/Def):** no âmbito do MD e das Forças Singulares (FS), é a equipe de prevenção, tratamento e resposta a incidentes cibernéticos operada pelo Comando de Defesa Cibernética (ComDCiber), na condição de órgão central do Sistema Militar de Defesa Cibernética, responsável pela articulação com o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo;

l) **Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR):** grupo de agentes públicos com a responsabilidade de prestar serviços relacionados à segurança cibernética para o órgão ou a entidade da Administração Pública Federal (APF), em observância à política de segurança da informação e aos processos de gestão de riscos de segurança da informação do órgão ou da entidade. Anteriormente era chamada de Equipe de Tratamento de Incidentes de Rede;

m) **gestão de continuidade de negócios em segurança da informação**: processo que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Esse processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação, a marca da organização e suas atividades de valor agregado;

n) **gestão de riscos em segurança da informação**: processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificação, avaliação e gerenciamento de potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos;

o) **integridade**: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

p) **Rede Operacional de Defesa (ROD):** rede de computadores fornecedora de serviços de comunicações de dados militares operacionais, compondo o SISMC^2. Está estruturada como uma *Wide Area Network* (WAN), com conectividade segregada (restrita, segura e controlada) e diversificada, por meio do SISCOMIS, das redes de dados das FS (RECIM, EBNET e INTRAER) e da *Internet*;

q) **resiliência**: capacidade de uma organização ou de uma infraestrutura de resistir aos efeitos de um incidente, ataque ou desastre, e retornar à normalidade das operações;

r) **segurança cibernética**: ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético, capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis;

s) **segurança da informação (SI):** consiste no conjunto de ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade em todo seu ciclo de vida;

t) **SISMC^2**: é o conjunto de instalações, equipamentos, sistemas de informação, comunicações, doutrinas, procedimentos e pessoal essenciais ao C^2, visando a atender ao preparo e ao emprego das Forças Armadas (FA). Abrange os sistemas Militares de C^2 das FA, bem como, outros sob a responsabilidade do MD;

u) **tratamento da informação**: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;

v) **risco**: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização; e

w) **não repúdio ou irretratabilidade**: capacidade de comprovar a ocorrência de um evento ou ação declarada e suas camadas originárias (camada física ou camada lógica).

CAPÍTULO III

ESCOPO

3.1 Abrangência

3.1.1 Para os fins do disposto nesta Política, a SI abrange:

a) segurança cibernética;
b) defesa cibernética; e
c) segurança física e a proteção de dados organizacionais.

3.1.2 A regulamentação da SI compreende um conjunto de diretrizes e normas a serem seguidos por todos os componentes do SISMC², em conformidade com os propósitos estabelecidos neste documento.

3.1.3 As informações que tramitam pelo SISMC², sob custódia do EMCFA e dos demais órgãos integrantes, exigem regulamentação específica para a sua proteção, uma vez que constituem recursos essenciais para o funcionamento da Estrutura Militar de Defesa (Etta Mi D), devendo ser protegidas e preservadas, por meio de atividades de SI.

3.1.4 Esta Política se aplica a todos os componentes dos sistemas de informação do SISMC², para o conhecimento, o planejamento, o preparo e a execução de ações de SI visando à garantia da disponibilidade, da integridade, da confidencialidade e da autenticidade das informações que trafegam pelo referido Sistema.

3.1.5 A POSIN-SISMC² orienta o tratamento da informação no âmbito da SISMC², em todo o seu ciclo de vida (criação, coleta, manuseio, divulgação, armazenamento, retenção, processamento, compartilhamento e eliminação), considerando a privacidade e a segurança desde a concepção e por padrão, visando à continuidade, em especial, das atividades críticas, em conformidade com a legislação vigente, normas, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de SI.

3.2 Objetivos

3.2.1 A POSIN-SISMC² tem por objetivos:

3.2.1.1 - Garantir a disponibilidade, integridade, confidencialidade e autenticidade da informação em seus suportes (pessoas, documentos, material, meios de Tecnologia da Informação (TI), áreas e instalações) pertencentes ou custodiados ao SISMC².

3.2.1.2 - Contribuir para o aumento da resiliência do SISMC².

3.2.1.3 - Promover o alinhamento das ações de SI ao planejamento estratégico da evolução do SISMC².

3.2.1.4 - Contribuir com a gestão de riscos em SI.

3.2.1.5 - Orientar a gestão de continuidade de negócios, no tocante à SI, no âmbito do SISMC².

3.2.1.6 - Aprimorar o sistema de auditoria de SI.

3.2.1.7 - Assegurar a irretratabilidade das ações praticadas pelos responsáveis por sistemas de informação integrantes do SISMC².

3.2.1.8 - Desenvolver e manter em permanente aprimoramento a cultura organizacional de SI em todos os níveis.

3.2.1.9 - Aprimorar a gestão de recursos humanos (processo seletivo, capacitação, desempenho da função, manutenção na atividade e desligamento) envolvidos no tratamento da informação.

3.2.1.10 - Aperfeiçoar processos e atualizar tecnologias no intuito de se obter um ambiente seguro para o trâmite da informação.

3.2.1.11 - Promover a interação com os demais órgãos da APF, comunidade acadêmica, institutos de pesquisa e infraestruturas críticas por meio da atuação colaborativa.

3.3 Atribuições

3.3.1 Cabe ao Subchefe de Comando e Controle (SCh de C²) da Chefia de Operações Conjuntas (CHOC):

a) assessorar o Ch de Op Cj na elaboração da Política de SI para o SISMC²;

b) exercer a coordenação do CD-SISMC²;

c) propor e coordenar a execução do planejamento estratégico do SISMC² correspondente à política de SI para o referido Sistema;

d) prover, aprimorar e manter em funcionamento seguro e ininterrupto a infraestrutura de C² sob responsabilidade da Subchefia de Comando e Controle (SC-1);

e) supervisionar, em apoio às operações conjuntas, as atividades relacionadas ao SISMC²; e

f) Coordenar as ações da ETIR da SC-1 (ETIR SC-1).

3.3.2 Cabe ao Encarregado de Segurança da Informação Setorial da CHOC:

a) assessorar, em caráter permanente, o SCh de C², nos trabalhos relativos à concepção, à organização, ao desenvolvimento, à implementação, à integração, à manutenção, à avaliação e a evolução das Normas, Técnicas e Procedimentos relativos a SI no SISMC²;

b) promover cultura de SI no âmbito da SC-1, por intermédio de atividades de sensibilização, conscientização, capacitação e especialização;

c) acompanhar as investigações e as avaliações dos danos decorrentes de incidentes porventura ocorridos nos ativos de informação que são de responsabilidade da SC-1;

d) propor alocação de recursos necessários às ações de SI;

e) coordenar a ETIR SC-1;

f) promover e acompanhar estudos de novas tecnologias, quanto a possíveis impactos SI no âmbito do SISMC^2;

g) manter contato permanente e estreito com o Gestor de Segurança da Informação da Administração Central do Ministério da Defesa (ACMD) e com os agentes responsáveis da ECS/Def e ETIR Centrais das FS, para o trato de assuntos relativos à SI; e

h) propor normas e procedimentos relativos à SI no âmbito do SISMC^2, em conformidade com as legislações existentes sobre o tema.

3.3.3 Cabe à ETIR SC-1:

a) realizar as atividades de prevenção, de tratamento e de resposta a incidentes cibernéticos no âmbito das atribuições regimentais da SC1;

b) priorizar a continuidade dos serviços de comunicações de dados militares operacionais fornecidos pela ROD;

c) realizar ações voltadas para o fortalecimento da resiliência cibernética do Centro de Comando e Controle do Ministério da Defesa (CC^{2}MD), órgão Central do SISMC^2;

d) comunicar a ECS/Def e às ETIR Centrais das FS, com a maior brevidade possível, a ocorrência de incidentes cibernéticos;

e) manter registro histórico de incidentes cibernéticos e vulnerabilidades que permitam a geração de dados estatísticos; e

f) cooperar com a ECS/Def, bem como com as ETIR Centrais das FS.

3.3.4 Cabe à ETIR Central das FS, sem prejuízo das demais competências previstas em normas específicas:

a) compartilhar alertas sobre ameaças e vulnerabilidades cibernéticas;

b) divulgar medidas de prevenção, tratamento e resposta a incidentes cibernéticos;

c) divulgar informações sobre ataques cibernéticos;

d) promover a cooperação entre os participantes do SISMC^2;

e) promover a celeridade na resposta a incidentes cibernéticos; e

f) comunicar imediatamente a ETIR SC-1 e à ECS/Def sobre a existência de vulnerabilidades ou incidentes cibernéticos mais relevantes e que comprometam, real ou potencialmente, a disponibilidade, da integridade, da confidencialidade e da autenticidade das informações inerentes aos serviços prestados ou contratados.

3.3.5 Cabe às FS, nos seus respectivos âmbitos de atuação:

a) em conformidade com o descrito Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, cabe designar um gestor de segurança da informação interno, indicado pela alta administração do órgão ou da entidade;

b) instituir comitê de segurança da informação ou estrutura equivalente, para deliberar sobre os assuntos relativos a esta Política;

c) estabelecer normas necessárias à efetiva implementação e manutenção da SI no âmbito do SISMC^2;

d) promover ações de capacitação e profissionalização dos recursos humanos empregados em proveito de temas relacionados à SI do SISMC^2;

e) instituir e implementar ETIR em redes computacionais; e
f) submeter à SC-1 as propostas de alterações desta Política.

3.3.6 Cabe aos usuários e custodiantes do SISMC²:

a) observar a presente Política e cumprir todas as normas e os procedimentos de SI vigentes;

b) tratar a informação como um ativo a ser protegido no contexto da Segurança/Defesa Nacional;

c) acessar os ativos de informação somente após tomar ciência da POSIN-SISMC² e assinar o Termo de Responsabilidade (Anexo B), atestando ter pleno conhecimento e aceitar expressamente, sem reservas, os termos da POSIN-SISMC²;

d) utilizar os ativos de informação, os sistemas e produtos computacionais de propriedade ou direito de uso exclusivamente para o interesse do serviço;

e) preservar o conteúdo das informações sigilosas a que tiver acesso, sem divulgá-las para pessoas não autorizadas e/ou que não tenham necessidade de conhecê-las;

f) proteger os ativos de informação contra acesso, modificação, destruição ou divulgação não autorizada;

g) usar exclusivamente a identificação para acesso próprio, não permitindo nem compartilhando, transferindo ou divulgando o conhecimento de credenciais de acesso de terceiros; e

h) estar ciente de que toda informação produzida, armazenada, processada e transmitida no âmbito do SISMC² pode ser auditada pelo setor competente do EMCFA.

3.4 Tráfego de Informações

3.4.1 As informações que tramitam pelo SISMC², sob custódia do EMCFA e dos outros órgãos integrantes, exigem regulamentação específica para sua proteção, uma vez que constituem recurso essencial para o funcionamento da Etta Mi D, devendo ser protegidas e preservadas por meio de ações de SI. Nesse contexto, o tráfego de informações controladas deverá ser realizado de acordo com as seguintes orientações gerais:

a) priorizar o tráfego de informações sigilosas por meio da ROD e rede das FS;

b) empregar sistemas criptográficos para a proteção de documentos considerados sigilosos, por meio do uso de sistemas de informações que utilizem criptografia de Estado;

c) os sistemas de informações responsáveis pelo tráfego de informações sigilosas (dados, vídeo e voz) devem utilizar criptografia para proteção do canal de transmissão; e

d) os enlaces digitais, principalmente os satelitais, utilizados para as comunicações de dados militares operacionais, deverão buscar o emprego de recursos criptográficos adequados ao seu emprego operacional.

3.5 Regulamentação

3.5.1 A regulamentação da SI compreende um conjunto de diretrizes e normas emitidas pelo GSI/PR. O cumprimento das diretrizes e normas de SI é de responsabilidade de todos os componentes, permanentes ou eventuais, do SISMC².

3.5.2 A documentação normativa de órgão integrante, permanente ou temporário, do SISMC[2] sobre SI deve considerar esta Política como referência básica para a sua elaboração.

CAPÍTULO IV

ORIENTAÇÕES GERAIS

4.1 Pressupostos básicos

4.1.1 A informação é um recurso vital para o adequado funcionamento de toda e qualquer organização, devendo ser tratada como patrimônio a ser protegido e preservado.

4.1.2 O sucesso das ações nos assuntos de SI está diretamente associado à capacitação científico-tecnológica dos recursos humanos envolvidos, à conscientização do público interno, à qualidade das soluções adotadas e à proteção das informações contra ameaças internas e externas.

4.1.3 O sigilo das informações é responsabilidade de todos que a elas tenham acesso.

4.1.4 Os integrantes do SISMC^2 devem zelar pela segurança física e do ambiente de suas instalações, bem como pela segurança dos dados organizacionais sob sua responsabilidade.

4.2 Tratamento da informação

4.2.1 Toda informação tratada por usuário, no exercício de suas atividades, é considerada bem e propriedade do SISMC^2 e deve ser protegida segundo as diretrizes descritas nesta publicação.

4.2.2 É expressamente proibido o acesso, a guarda ou o encaminhamento de material discriminatório, malicioso, não ético, obsceno ou ilegal por intermédio de quaisquer meios e recursos de tecnologia da informação disponibilizados pela ROD.

4.2.3 Os ativos de informação devem ser protegidos de modo preventivo, com o objetivo de reduzir ameaças e minimizar riscos às atividades de C^2 das operações militares.

4.2.4 No tratamento das informações, deve-se respeitar a classificação segundo o grau de sigilo, o aspecto crítico e a proteção de dados pessoais, conforme normas internas e legislação específica em vigor.

4.2.5 A manipulação e a eliminação de informações classificadas em qualquer grau de sigilo devem seguir as normas internas e a legislação em vigor.

4.2.6 Os responsáveis pelos ativos de informação devem manter registros e procedimentos que assegurem o rastreamento, o acompanhamento, o controle e a verificação de acesso, em especial aos sistemas corporativos e às redes computacionais.

4.3 Gestão de ativos

4.3.1 Nos aspectos relacionados à SI, o mapeamento de ativos de informação e o correspondente inventário devem produzir subsídios para a gestão de incidentes de SI, de riscos e de continuidade, bem como para os procedimentos de avaliação da conformidade, de melhorias contínuas, de auditoria e, principalmente, de estruturação e de administração da base de dados sobre os ativos de informação.

4.4 Gestão de continuidade de negócios em Segurança da Informação

4.4.1 A implementação do processo de gestão de continuidade de negócios tem o objetivo de minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas, além de recuperar perdas de ativos de informação em nível aceitável, por intermédio de ações de resposta a incidentes e recuperação de desastres.

4.4.2 O processo de gestão de continuidade de negócios deve se basear em um plano de continuidade de SI, estruturado a partir da análise e avaliação dos riscos de SI identificados e da prioridade de recuperação dos ativos de informação.

4.4.3 O Encarregado de Segurança da Informação Setorial da CHOC coordenará o processo de gestão de continuidade em SI dos ativos de informação sob responsabilidade do MD.

4.4.4 Conforme descrito na alínea a) do item 3.3.5, o gestor de segurança da informação designado, será o responsável pela gestão de continuidade em SI, no que concerne ao SISMC^2, sob responsabilidade da respectiva FS.

4.5 Gestão do uso de recursos operacionais e de comunicações

4.5.1 O uso de recursos operacionais e de comunicações deve seguir procedimentos estabelecidos pelas áreas competentes em conformidade com a POSIN-SISMC^2 e observando, no mínimo, o seguinte:

a) o correio eletrônico institucional é um meio de comunicações oficial e deve ser utilizado exclusivamente no desempenho das atividades funcionais;

b) o acesso à Internet provido pelo SISMC^2 deve ter seu uso disciplinado para a restrita execução das atividades funcionais;

c) o uso de dispositivos móveis de armazenamento deve ser controlado com a implementação de mecanismos de autenticação, autorização e registro de acesso do usuário;

d) é vedado o uso de redes sociais, tais como, *Facebook*, *Instagram*, *WhatsApp*, *Telegram* e *X* a partir de estações de trabalho conectadas à ROD, por esta ser uma rede para fins operacionais. Os usuários que, de acordo com o seu exercício funcional, tiverem a necessidade de acesso às mídias e redes sociais a partir de estações de trabalho conectadas à ROD, deverão ter autorização concedida pelo SCh de C^2;

e) a implementação ou contratação de computação em nuvem deve ser precedida de procedimentos de conformidade com a legislação vigente;

f) as informações classificadas em qualquer grau de sigilo devem ser protegidas mediante o emprego de recurso criptográfico adequado; e

g) as tabelas que armazenam senha de acesso e autenticação devem ser criptografadas.

4.6 Controle de acesso

4.6.1 O controle de acesso aos ativos de informação e às áreas e instalações deve ser implantado nos níveis físico e lógico, conforme procedimentos estabelecidos pelas áreas competentes.

4.6.2 O controle de acesso aos ativos de informação deverá conter identificador único, pessoal, intransferível e com validade estabelecida, que permita de maneira clara e indiscutível o seu reconhecimento.

4.7 Auditoria e conformidade

4.7.1 Os custodiantes de ativos da informação devem estabelecer procedimentos de auditoria, com objetivo de averiguar se estão de acordo com as legislações, normas e procedimentos relacionados à SI em sua área de competência.

4.7.2 A avaliação de conformidade nos aspectos de SI visa proporcionar adequado grau de confiança a um determinado processo, mediante o atendimento de requisitos definidos em políticas, procedimentos, normas ou em regulamentos técnicos aplicáveis.

4.7.3 O processo de avaliação de conformidade nos aspectos de SI deve ser composto pelo plano de verificação de conformidade e pelo relatório de avaliação de conformidade, que serão elaborados pelos custodiantes dos ativos de informação.

4.7.4 As auditorias devem ser realizadas, no mínimo, anualmente, para verificar a conformidade e a efetividade dos controles de SI implantados no SISMC². Todos os usuários estão sujeitos à auditoria e fiscalização ao utilizar os recursos do SISMC².

4.7.5 O descumprimento ou a violação desta Política de Segurança da Informação e demais normas e procedimentos estabelecidos relativos a ela terá implicação administrativa, civil e penal, segundo as normas e a legislação vigentes, de acordo com a gravidade do ato praticado.

4.8 Contratação de serviços

4.8.1 Nos editais de licitação e nos contratos deverá constar cláusula específica sobre a obrigatoriedade de atendimento às normas da POSIN-SISMC², bem como ser exigida da empresa contratada e do prestador de serviços a assinatura do Termo de Responsabilidade (Anexo B) e do Termo de Compromisso de Manutenção de Sigilo (Anexo C), quando aplicável.

4.8.2 A empresa contratada também deverá manter mecanismos que garantam a segurança das informações por ela acessadas direta ou indiretamente.

4.8.3 A gestão de processos de tecnologia da informação ou a gestão de SI não poderá ser objeto de contratação para execução de forma indireta.

4.9 Segurança física e do ambiente

4.9.1 Os responsáveis pela segurança física e do ambiente deverão estabelecer os perímetros de segurança, regras de controle de acesso e aspectos de monitoramento, bem como outras medidas visando à segurança física e do ambiente.

4.10 Gestão de incidentes de segurança da informação

4.10.1 A criação, a estrutura e o modelo de implementação da(s) ETIR serão definidos em conformidade com as diretrizes do GSI/PR.

4.10.2 Os incidentes que afetem dados pessoais deverão ser imediatamente comunicados ao Encarregado pelo Tratamento de Dados Pessoais da organização, que orientará sobre as práticas a serem adotadas.

4.10.3 Os custodiantes da informação realizarão a gestão de incidentes envolvendo a segurança física e do ambiente.

4.10.4 Todos os órgãos integrantes, permanentes ou temporários, do SISMC[2] zelarão pela gestão dos dados organizacionais sob sua responsabilidade.

4.11 Gestão de risco

4.11.1 Risco de segurança da informação está associado à exploração de uma ou mais vulnerabilidades de um ou mais ativos de informação, devendo ser continuamente monitorado e tratado, conforme legislação em vigor.

CAPÍTULO V

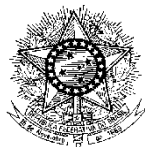
DISPOSIÇÕES FINAIS

5.1 Atualização

Esta Política e seus instrumentos normativos derivados deverão ser revisados sempre que se fizer necessário, com apoio de representantes dos setores especializados das três Forças Singulares, não excedendo o período máximo de quatro anos de sua promulgação.

ANEXO A
LISTA DE SIGLAS, ABREVIATURAS E ACRÔNIMOS

CD-SISMC^2	Conselho Diretor do Sistema Militar de Comando e Controle
Ch de Op Cj	Chefe de Operações Conjuntas
EBNET	Rede Corporativa Privativa do Exército
e-Ciber	Estratégia Nacional de Segurança Cibernética
ECS/Def	Equipe de Coordenação Setorial Defesa
ETIR	Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos
ETIR SC-1	Equipe de Prevenção, Tratamento e Resposta de Incidentes Cibernéticos da Subchefia de Comando e Controle
INTRAER	Rede Coorporativa Interna da Aeronáutica
LGPD	Lei Geral de Proteção de Dados
PNSI	Política Nacional de Segurança da Informação
POSIN-SISMC^2	Política de Segurança da Informação para o Sistema Militar de Comando e Controle
RECIM	Rede de Comunicações Integrada da Marinha
ReGIC	Rede Federal de Gestão de Incidentes Cibernéticos
SCh de C^2	Subchefe de Comando e Controle
SI	Segurança da Informação
WAN	*Wide Area Network*

ANEXO B

MINISTÉRIO DA DEFESA
CHEFIA DE OPERAÇÕES CONJUNTAS
SUBCHEFIA DE COMANDO E CONTROLE

MODELO DE TERMO DE RESPONSABILIDADE

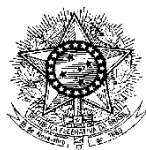
Pelo presente instrumento, eu, ____CPF nº ___________ lotado(a) no(a)____________________________,na qualidade de USUÁRIO (A) da Rede Operacional de Defesa (ROD) ou CUSTODIANTE de informações da ROD, declaro ter conhecimento da Política de Segurança da Informação para o Sistema Militar de Comando e Controle (POSIN-SISMC[2]), segundo a qual, sem restar qualquer dúvida de minha parte, devo cumprir todas as suas diretrizes e orientações.
Estou ciente de meu compromisso com o Ministério da Defesa e assumo a responsabilidade pelas consequências decorrentes da não observância do disposto na POSIN-SISMC[2] e na legislação vigente.

Aviso de Privacidade

Suas informações serão coletadas para fins de acesso aos ativos da ROD ou para responsabilização legal, atendendo aos princípios da finalidade e da necessidade segundo a LGPD.
Os seus dados pessoais serão armazenados e tratados no território nacional. O tempo de guarda e de eliminação dos dados seguem o disposto na Política Nacional de Arquivos Públicos (Lei nº 8.159/1991), no Decreto nº 7845/2012 e na Portaria GM-MD nº 5.814, de 29 de novembro de 2022.

Brasília/DF, _______ de _______________ de _________

____
Assinatura
(Usuário ou custodiante da informação)

ANEXO C

MINISTÉRIO DA DEFESA
CHEFIA DE OPERAÇÕES CONJUNTAS
SUBCHEFIA DE COMANDO E CONTROLE

MODELO DE TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

Pelo presente instrumento, eu, ____ CPF nº____________________representante legal da empresa____ inscrita no CNPJ sob o nº ____________________________________ sediada em______________________________ para fins da execução do contrato nº ___________________________ comprometo-me a manter em sigilo, ou seja, não revelar ou divulgar as informações sigilosas ou de caráter não público recebidas durante e após o exercício funcional ou prestação de serviços no âmbito da Rede Operacional de Defesa (ROD).

A duração do período de sigilo e confidencialidades será a partir do momento de assinatura deste termo.

Mesmo após a finalização da prestação de serviços/negociação os dados deverão ser mantidos em confidencialidade não podendo ser compartilhados com terceiros e/ou qualquer outrem sem autorização da parte proprietária das informações.

A violação dos termos deste instrumento resultará na aplicação das penalidades previstas em lei, nos âmbitos administrativo, civil, penal e militar.

Aviso de Privacidade

Suas informações serão coletadas para fins de acesso aos ativos da ROD ou para responsabilização legal, atendendo aos princípios da finalidade e da necessidade segundo a LGPD.
Os seus dados pessoais serão armazenados e tratados no território nacional. O tempo de guarda e de eliminação dos dados seguem o disposto na Política Nacional de Arquivos Públicos (Lei nº 8.159/1991), no Decreto nº 7845/2012 e na Portaria GM-MD nº 5.814, de 29 de novembro de 2022.

Brasília/DF, _______ de _______________ de _________

____
Assinatura

Ministério da Defesa
Estado-Maior Conjunto das Forças Armadas
Brasília, 20 de novembro de 2023